

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-134189

(43)Date of publication of application : 21.05.1999

(51)Int.Cl.

G06F 9/06

G06F 12/14

G06K 19/10

(21)Application number : 09-298446

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 30.10.1997

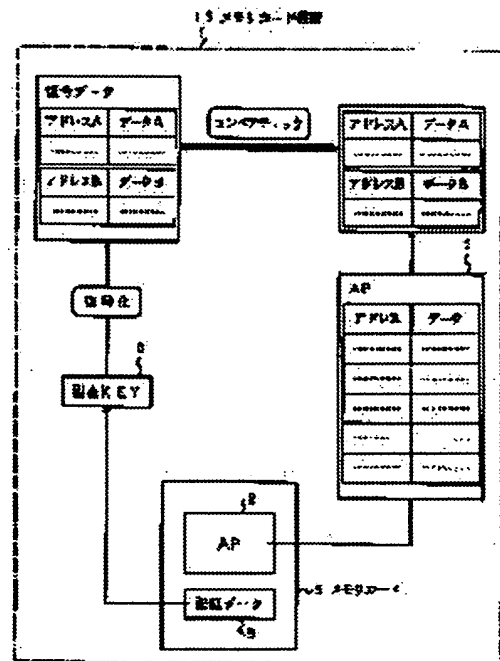
(72)Inventor : HARADA SEIICHI

(54) MEMORY CARD, AUTHENTICATION DATA GENERATION DEVICE AND MEMORY CARD DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a memory card device checking the truth or false of a memory card before an application program is executed and to provide a authentication data generation device for generation authentication data used for checking the truth or false and storing it in the memory card.

SOLUTION: Authentication data 9 obtained by ciphering an address which is read from the application program 2 at random and data stored in the address by a secret key 8 is stored in the memory card 5. Authentication data 9 is read from the memory card 5 and it is decoded by the secret key 8. Data which is read from the application program 2 based on the decoded address is compared with decoded data and the truth or false of the memory card 5 is checked.



LEGAL STATUS

[Date of request for examination] 29.02.2000

[Date of sending the examiner's decision of rejection] 21.10.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2003-22503

[Date of requesting appeal against examiner's decision of rejection] 20.11.2003

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-134189

(43) 公開日 平成11年(1999) 5月21日

(51) Int.Cl.⁸

G 0 6 F 9/06

識別記号

5 5 0

F I

G 0 6 F 9/06

5 5 0 B

5 5 0 G

12/14

3 2 0

12/14

3 2 0 B

G 0 6 K 19/10

G 0 6 K 19/00

R

審査請求 未請求 請求項の数10 O L (全 13 頁)

(21) 出願番号

特願平9-298446

(22) 出願日

平成9年(1997)10月30日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 原田 聖一

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

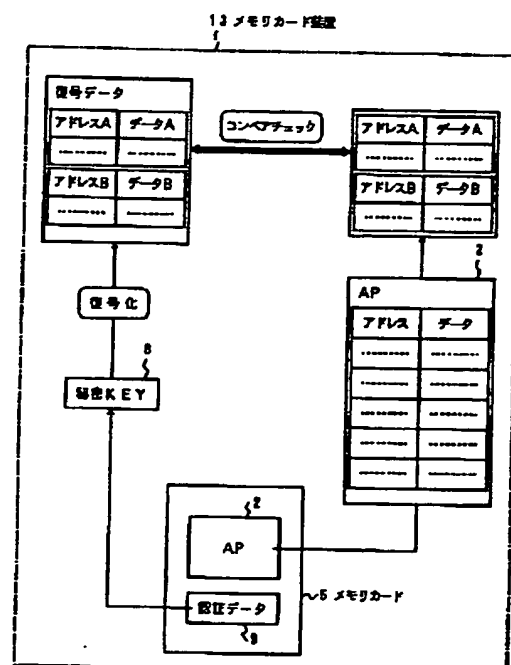
(74) 代理人 弁理士 大西 健治

(54) 【発明の名称】 メモリカードと認証データ作成装置とメモリカード装置

(57) 【要約】

【課題】 アプリケーションプログラムを実行する前にメモリカードの真偽をチェックできるメモリカード装置と、その真偽のチェックに用いる認証データを作成してメモリカードに格納する認証データ作成装置とを提供する。

【解決手段】 アプリケーションプログラム2からランダムに読み出されたアドレスとそのアドレスに格納されたデータとを秘密キー8により暗号化した認証データ9をメモリカード5に格納し、メモリカード5から認証データ9を読み出して秘密キー8により復号化し、復号化されたアドレスに基づきアプリケーションプログラム2から読み出したデータと復号化されたデータとを比較してメモリカード5の真偽をチェックする。



メモリカード認証動作の説明図(1)

【特許請求の範囲】

【請求項 1】 メモリカード装置に実装されるアプリケーションプログラムを格納したメモリカードにおいて、メモリカードの真偽チェックに用いる暗号化された認証データを格納していることを特徴としたメモリカード。

【請求項 2】 請求項 1 に記載したメモリカードの認証データを作成する認証データ作成装置であって、上記アプリケーションプログラムからランダムに読み出されたアドレスと該アドレスに格納されたデータとを秘密キーにより暗号化した認証データを上記メモリカードに格納することを特徴とした認証データ作成装置。

【請求項 3】 上記秘密キーは、ランダムに読み出された上記アドレスを認証アドレスに暗号化するとともに該アドレスに格納されたデータを認証ハッシュ値に変換する請求項 2 記載の認証データ作成装置。

【請求項 4】 メモリカードに格納されるアプリケーションプログラムからランダムに読み出されたアドレスと該アドレスに格納されたデータとを秘密キーにより暗号化した認証データを格納したメモリカードを実装するメモリカード装置であって、上記メモリカードから認証データを読み出して上記秘密キーにより復号化し、復号化されたアドレスに基づき上記アプリケーションプログラムから読み出したデータと復号化されたデータとを比較してメモリカードの真偽をチェックすることを特徴とするメモリカード装置。

【請求項 5】 上記認証データは、ランダムに読み出された上記アドレスを上記秘密キーにより暗号化した認証アドレスと、該アドレスに格納されたデータを上記秘密キーにより変換した認証ハッシュ値とからなり、認証アドレスを上記秘密キーにより復号化するとともに復号化されたアドレスに基づき上記アプリケーションプログラムから読み出されたデータを比較ハッシュ値に変換し、該比較ハッシュ値と上記認証ハッシュ値とを比較してメモリカードの真偽をチェックする請求項 4 記載のメモリカード装置。

【請求項 6】 リセットボタンの押下により上記メモリカードの真偽の認証処理を行い、該メモリカードが真の場合には装置のメモリに認証 OK フラグデータをセットし、以後、電源ボタン押下により上記認証 OK フラグデータのセット状態をチェックし、セットならば該メモリカードを真と認証する請求項 4 記載、又は請求項 5 記載のメモリカード装置。

【請求項 7】 リセットボタンの押下により上記メモリカードの真偽の認証処理を行い、該メモリカードが真の場合には装置のメモリに認証 OK フラグデータをセットするとともにメモリカードの認証データをクリアし、以後、電源ボタン押下により上記認証 OK フラグデータのセット状態をチェックし、セットならば該メモリカードを真と認証する請求項 4 記載、又は請求項 5 記載のメモリカード装置。

【請求項 8】 電源ボタンを押下する毎に上記メモリカードの真偽の認証処理を行う請求項 4 記載のメモリカード装置。

【請求項 9】 待ち状態が予め決められた時間経過すると、装置を低消費電力モードに切り替える請求項 4 記載、又は請求項 5 記載のメモリカード装置。

【請求項 10】 上記メモリカードが装置から抜去された場合には装置のメモリにセットされた上記認証フラグをクリアする請求項 4 記載、又は請求項 5 記載のメモリカード装置。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は電子商取引に使用される携帯型電子機器等のメモリカードを使用するメモリカード装置と、そのメモリカードに格納する認証データを作成する認証データ作成装置とに関する。

【0002】

【従来の技術】 従来、メモリカード装置、例えば、電子商取引に使用される携帯型電子機器では、アプリケーションプログラムが格納されてあるメモリカードをメモリカード装置に挿入すると、アプリケーションプログラムが即、実行される。

【0003】

【発明が解決しようとする課題】 従来のメモリカード装置にあつては、メモリカードの真偽をチェックする機能が設けてないので、メモリカードがメモリカード装置に挿入されると、たとえ不正なアプリケーションプログラムが実装してあつても実行されてしまい、電子商取引の内容が書き替えられてしまう恐れがあるという問題点があつた。

【0004】 本発明はアプリケーションプログラムを実行する前にメモリカードの真偽をチェックできるメモリカード装置と、その真偽のチェックに用いる認証データを作成してメモリカードに格納する認証データ作成装置とを提供することを目的としている。

【0005】

【課題を解決するための手段】 上記目的を達成するために本発明は、アプリケーションプログラムからランダムに読み出されたアドレスと該アドレスに格納されたデータとを秘密キーにより暗号化した認証データをメモリカードに格納する認証データ作成装置と、メモリカードから認証データを読み出して秘密キーにより復号化し、復号化されたアドレスに基づきアプリケーションプログラムから読み出したデータと復号化されたデータとを比較してメモリカードの真偽をチェックするメモリカード装置とを備える。

【0006】

【発明の実施の形態】 本発明の実施の形態について図面を参照しながら説明する。尚、各図面に共通な要素には同一符号を付す。

第1の実施の形態

図2はメモリカードライタの構成を示すブロック図である。メモリカードライタ1は、後述するメモリカード装置で実行されるアプリケーションプログラム2（以後AP2と記す）を格納した媒体3（以後AP媒体3と記す）を挿抜するAP用I/Oスロット4と、メモリカード5を挿抜するメモリカード接続用I/Oスロット6と、書き込み開始スイッチ7とを有する。

【0007】AP媒体3、メモリカード5はAP用I/Oスロット4、メモリカード接続用I/Oスロット6に設けられた図示せぬコネクタに挿抜する端子部3a、5aを有する。

【0008】メモリカードライタ1には、AP2の実行コードから、例えば1KB（キロバイト）程度のアドレスとデータとのセットをランダムに選択し、そのセットデータを秘密キー8（以後秘密KEY8と記す）を用いて暗号化し、認証データ9としてメモリカード5に格納する認証データ作成手段10と、AP2をメモリカード5に書き込むAP書き込み手段11とを内蔵している。

【0009】具体的には、図示せぬメモリに格納してある認証データ作成プログラム、AP書き込みプログラムをCPU12が実行することによって各手段を達成する。

【0010】アドレスとデータとのセットをランダムに選択するには、例えば、乱数を発生させ、その乱数でアドレスを構成してデータを選択するプログラムを認証データ作成プログラムに含ませておく。

【0011】図3はメモリカード装置の外観斜視図、図4は図3に示したメモリカード装置に搭載される制御ブロック図である。メモリカード装置13、例えば、電子商取引に使用される携帯型電子機器は、表面に操作キー群14、表示部15を備えてある。側面には矢印A-B方向にメモリカード5を挿抜する際に用いるメモリカード挿入口16及びメモリカード挿入口16に挿入した際メモリカード5をロックする矢印C-D方向に移動自在なスライダ17を有する。

【0012】操作キー群14には電源ボタン14a、リセットボタン14b、テンキー等があり、表示部15には操作に伴うメッセージが表示される。

【0013】メモリカード装置13の内部には、メモリカード挿入口16から挿入されるメモリカード5と並行になるように、破線で示す基板18が搭載してある。基板18には、図4に示すように、中央処理装置19（以後CPU19と記す）、ROM20、RAM21、バッテリー22等が搭載されてある。バッテリー22はCPU19、ROM20、RAM21にライン23を通じて電力を供給し、CPU19はROM20、RAM21とバスライン24で接続されている。

【0014】ROM20には制御プログラム20a、認証プログラム20b、秘密キー8（以後秘密KEY8と

記す）が格納してあり、RAM21はメモリカード5から読み込まれたAP2の格納や各種処理時のデータ格納に用いられる。秘密KEY8はメモリカード5の認証データ9を復号化する際に用いられるもので外部からの読み出しに対しプロテクトされてある。

【0015】CPU19は認証プログラム20bを実行することによりメモリカード認証手段26となり、メモリカード5が真の場合には表示部15に「APの実行に移る」旨のメッセージを表示するとともに、RAM21にメモリカード5が真であることを示す認証OKフラグデータ21aをセットする。

【0016】また、CPU19は制御プログラム20aを実行することによりタイマ手段25、低電力消費モード切替手段27、カード実装チェック手段28、カード引き抜きチェック手段29等になる。

【0017】低電力消費モード切替手段27はタイマ手段25を用い、待ち状態が予め決められた時間経過すると、CPU19をホールド状態に切り替え、無駄な電力消費を抑える。カード実装チェック手段28はメモリカード5の端子部5aが差し込まれるコネクタの状況を表すレジスタの内容をタイマ手段25を用い、例えば1秒割り込みで確認する。

【0018】また、スライダ17を矢印D方向に移動させると、マスク不可能な割り込み信号（NMI）がCPU19に送られ、カード引き抜きチェック手段29がRAM21の認証OKフラグデータ21aをクリアする。

【0019】次に動作について説明する。先ず、図5を参照してメモリカードライタ1の動作について説明する。AP2を格納したAP媒体3、何も書き込まれていないメモリカード5を、それぞれ、AP用I/Oスロット4、メモリカード接続用I/Oスロット6に挿入し、書き込み開始スイッチ7を押下する。

【0020】CPU12はAP書き込み手段11としてAP媒体3からAP2を読み込み、メモリカード5に書き込む。

【0021】次に、CPU12は認証データ作成手段10としてAP2からアドレスとデータとのセット2aをランダムに選択し、そのセットデータ2aを秘密KEY8を用いて暗号化し、認証データ9としてメモリカード5に書き込む。

【0022】次に、図1、図6を参照してメモリカード認証動作について説明する。図1は第1の実施の形態によるメモリカード認証動作の説明図（1）、図6は第1の実施の形態によるリセットボタン押下後の動作を示すフローチャート（1）である。メモリカード5の端子部5aをメモリカード装置13のメモリカード挿入口16から矢印A方向へ挿入する。端子部5aはメモリカード装置13の内部に設けられた図示せぬコネクタに差し込まれる。

【0023】メモリカード5には、メモリカードライタ

1によりAP2、認証データ9が格納されてある。リセットボタン14bが押下されると、ステップS1でCPU19は制御プログラム20aに基づきメモリカード装置13を初期化する。初期化によって、RAM21の認証OKフラグデータ21aもクリアされる。

【0024】ステップS2でCPU19はメモリカード認証手段26として、図1に示すように、メモリカード5からAP2を読み出し、RAM21に格納する。ステップS3でメモリカード5から認証データ9を読み出し、秘密KEY8を用いて復号化し、復号データとしてRAM21に格納する。

【0025】ステップS4で復号データのアドレスに基づいてRAM21に格納してあるAP2からデータを読み出す。即ち、CPU19は復号データのアドレスを図示せぬプログラムカウンタに入力し、RAM21に格納してあるAP2からデータを読み出す。

【0026】ステップS5でAP2から読み出したデータと復号データのデータとを比較する。即ち、CPU19はAP2から読み出したデータと復号データのデータとを図示せぬ演算部のレジスタにセットして比較する。ステップS6で一致ならばステップS7に分岐し、否ならばステップS9に分岐する。

【0027】ステップS7で比較するデータが未だ有るか否かをチェックし、有ればステップS5に分岐し、否ならばステップS8に分岐する。ステップS8でCPU19は表示部15に「APの実行に移る」旨のメッセージを表示するとともに、RAM21に認証OKフラグデータ21aをセットし、メモリカード認証動作を終了する。

【0028】ステップS9でCPU19は表示部15に「メモリカードは不正である」旨のメッセージを表示してメモリカード認証動作を終了する。

【0029】次に図7を参照して電源ボタン押下後の動作を説明する。図7は第1の実施の形態による電源ボタン押下後の動作を示すフローチャート(1)である。電源ボタン14aが押下されると、ステップS10でCPU19はメモリカード認証手段26として、RAM21の認証OKフラグデータ21aがセットされているか否かをチェックし、セットされていればステップS11に分岐し、否ならばステップS12に分岐する。

【0030】ステップS11でCPU19は表示部15に「APの実行に移る」旨のメッセージを表示し、メモリカード認証動作を終了する。ステップS12でCPU19は表示部15に「メモリカードは不正である」旨のメッセージを表示し、メモリカード認証動作を終了する。

【0031】次に図8を参照してカード引き抜き後の動作を説明する。メモリカード認証動作は終了してRAM21に認証OKフラグデータ21aがセットされている。メモリカード5を引き抜くためにスライダ17を矢印D方向に移動させると、ステップS20でCPU19は

カード引き抜きチェック手段29としてマスク不可能な割り込み信号(NMI)が発生したか否かをセンスしており、発生ならばステップS21に分岐する。ステップS21でRAM21の認証OKフラグデータ21aをクリアするとともに表示部15に「認証OKフラグデータをクリアした」旨のメッセージを表示して処理を終了する。従って、次回APを実行させるには、リセットボタン14bを押下しなければならない。

【0032】第1の実施の形態によれば、メモリカードライタを装置ベンダーから信頼できるユーザ(システムベンダー、ソフトハウス等)に提供、管理させることでユーザライタブルでしかも、セキュリティを持ったメモリカードの提供が可能なシステムを実現できる。

【0033】また、APの実行コードのアドレスとデータとからなるセットデータを暗号化して認証データを作成してメモリカードに格納し、メモリカード装置で認証データを復号化し、APと比較してメモリカードの真偽をチェックできるようにしたので、不正なAPが実行される恐れはなくなる。

【0034】また、メモリカード装置にAPに関する情報が実装されていなくともメモリカードの真偽がチェックできるので、APのバージョンアップ等の変更が生じても、メモリカード装置側では何の変更も伴わず、変更後のメモリカードの真偽をチェックできる。

【0035】また、リセットボタン押下に伴うメモリカードの真偽チェックで真と判定されれば、以後、電源ボタン押下に伴う認証OKフラグデータのチェックでメモリカードの真偽チェックを行えるので、真偽チェックに要する時間を短縮できる。

【0036】また、メモリカード装置からメモリカードが引き抜かれた場合、認証OKフラグデータをクリアするようにしたことにより、その後、偽造メモリカードをメモリカード装置に実装し、電源ボタンを押下しても「メモリカードは不正である」旨のメッセージを表示されるので、偽造メモリカードの使用を防止できる。

【0037】第2の実施の形態

第2の実施の形態が第1の実施の形態と異なるところは、電源ボタンがリセットボタンをも兼ねている点と、メモリカード認証手段がRAM21に認証OKフラグデータ21aをセットしない点である。

【0038】図9は第2の実施の形態によるフローチャートである。第1の実施の形態のメモリカード認証動作と異なるところは、電源ボタン14aが押下される毎に、CPU19はリセットされ、ステップS1でメモリカード装置13を初期化する点と、ステップS8でRAM21に認証OKフラグデータ21aをセットしない点である。

【0039】第2の実施の形態によれば、メモリカード装置を立ち上げる(電源ボタンを押下する)毎に、CPUはメモリカードの認証動作を行うので、第1の実施の

形態による認証OKフラグデータセットに比べてセキュリティが向上し、不正なアプリケーションプログラムが実行される恐れはなくなる。

【0040】第3の実施の形態

第3の実施の形態が第1の実施の形態と異なるところは、リセットボタン押下により開始されるメモリカードの認証動作である。即ち、認証動作によりメモリカードが真であれば、RAM21に認証OKフラグデータ21aをセットするとともに、メモリカード2の認証データをクリア（例えば認証データに有効ビット、無効ビットを立てるようしておきメモリカードが真であれば無効ビットを立てる）にする点である。

【0041】動作については第1の実施の形態と同じであるから省略する。

【0042】第3の実施の形態によれば、AP認証後、メモリカードの認証データをクリアすることにより、一度認証されたメモリカード（又は、その不正コピー）を他のメモリカード装置で再利用することを不可能にし、さらに、メモリカード装置に実装されて出荷されたメモリカードからの読み出しを不可能にし、偽造メモリカードの製造を防止させることができる。

【0043】第4の実施の形態

第4の実施の形態が第1の実施の形態と異なるところは、メモリカードライタ1により認証データ9を作成する際、秘密KEYを用いてアドレスを認証アドレスに暗号化するとともにデータを認証ハッシュ値に変換する。

【0044】メモリカード装置13では、秘密KEYを用いて認証アドレスを復号化し、復号化されたアドレスに基づいてAPからデータを読み出し、秘密KEYを用いてデータから比較ハッシュ値を求め、認証ハッシュ値と比較してメモリカードの真偽をチェックする。

【0045】図10は第4の実施の形態によるメモリカードライタの動作を示す説明図である。先ず、図2に示したように、AP2を格納したAP媒体3、何も書き込まれていないメモリカード5を、それぞれ、AP用I/Oスロット4、メモリカード接続用I/Oスロット6に挿入し、書き込み開始スイッチ7を押下する。

【0046】CPU12はAP書き込み手段11として、図10に示すように、AP媒体3からAP2を読み込み、メモリカード5に書き込む。

【0047】次に、CPU12は認証データ作成手段10として、読み込んだAP2からアドレスとデータとのセットデータ2aをランダムに選択し、そのセットデータ2aと秘密KEY30とを用いて認証データ9を作成し、メモリカード5に書き込む。

【0048】セットデータ2aのうち、アドレスは秘密KEY30を用いて暗号化され、認証アドレス9aとしてメモリカード5に書き込まれる。同様に、データは秘密KEY30を用いてハッシュ値に変換され、認証ハッシュ値9bとしてメモリカード5に書き込まれる。

【0049】図11は第4の実施の形態によるメモリカード認証動作の説明図、図12は第4の実施の形態によるリセットボタン押下後の動作を示すフローチャート(2)である。

【0050】メモリカード5には、メモリカードライタ1によりAP2、認証データ9が格納されてある。リセットボタン14bが押下されると、ステップS1でCPU19は制御プログラム20aに基づきメモリカード装置13を初期化する。初期化によって、RAM21の認証OKフラグデータ21aもクリアされる。

【0051】ステップS2でCPU19はメモリカード認証手段26として、図11に示すように、メモリカード5からAP2を読み出し、RAM21に格納する。ステップS3でメモリカード5から認証アドレス9aを読み出し、秘密KEY30を用いて復号化し、復号アドレス31としてRAM21に格納する。

【0052】ステップS4で復号アドレス31に基づいてRAM21に格納してあるAP2からデータを読み出し、データ群32としてRAM21に格納する。即ち、CPU19は復号化されたアドレスを順に図示せぬプログラムカウンタに入力し、RAM21に格納してあるAP2からデータを読み出す。

【0053】ステップS5で秘密KEY30を用いてデータ群32からハッシュ値を算出し、比較ハッシュ値33としてRAM21に格納する。ステップS6でメモリカード5の認証ハッシュ値9bと比較ハッシュ値33とを比較する。即ち、CPU19は認証ハッシュ値9bと比較ハッシュ値33とをRAM21から図示せぬ演算部のレジスタにセットして比較する。ステップS7で一致ならばステップS8に分岐し、否ならばステップS10に分岐する。

【0054】ステップS8でCPU19は表示部15に「APの実行に移る」旨のメッセージを表示するとともに、RAM21に認証OKフラグデータ21aをセットし、メモリカード認証動作を終了する。

【0055】ステップS9でCPU19は表示部15に「メモリカードは不正である」旨のメッセージを表示してメモリカード認証動作を終了する。

【0056】第4の実施の形態によれば、データは最後のハッシュ値を認証ハッシュ値としてメモリカードに格納されるようにしたので、第1の実施の形態に比べてメモリカードに実装する認証データのサイズを大幅に小さくすることができる。

【0057】

【発明の効果】本発明は、以上説明したように構成されているので以下に記載される効果を奏する。アプリケーションプログラムと暗号化した認証データとを格納したメモリカードをメモリカード装置に実装し、認証データを復号化して得られたアドレスによりアプリケーションプログラムから読み出したデータ、あるいは読み出して

処理したデータと、認証データから得られたデータと比較してメモ리카ードの真偽をチェックするようにしたことにより、不正なアプリケーションプログラムを実装したメモ리카ードがメモ리카ード装置に挿入されても実行されないで、電子商取引の内容等が書き替えられてしまう恐れがなくなる。

【図面の簡単な説明】

【図 1】メモ리카ード認証動作の説明図 (1) である。

【図 2】メモ리카ードライタの構成を示すブロック図である。

【図 3】メモ리카ード装置の外観斜視図である。

【図 4】メモ리카ード装置に搭載される制御ブロック図である。

【図 5】メモ리카ードライタの動作を示す説明図 (1) である。

【図 6】リセットボタン押下後の動作を示すフローチャート (1) である。

【図 7】電源ボタン押下後の動作を示すフローチャート (1) である。

【図 8】カード引き抜き後の動作を示すフローチャートである。

【図 9】電源ボタン押下後の動作を示すフローチャート (2) である。

【図 10】メモ리카ードライタの動作を示す説明図 (2) である。

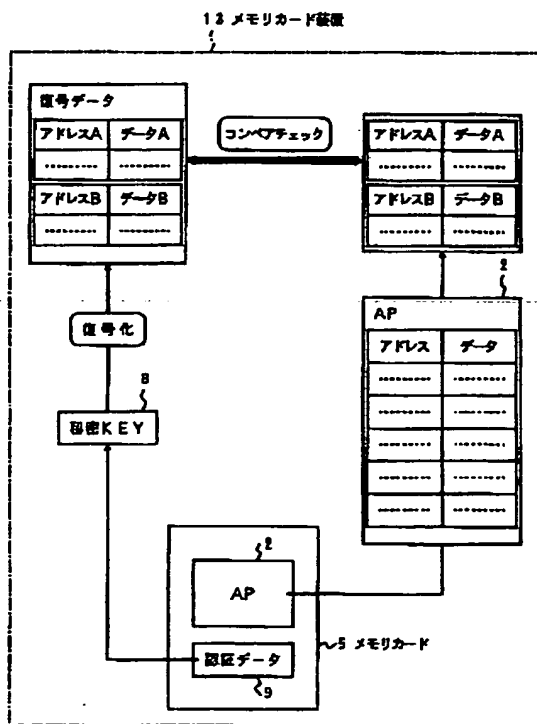
【図 11】メモ리카ード認証動作の説明図 (2) である。

【図 12】リセットボタン押下後の動作を示すフローチャート (2) である。

【符号の説明】

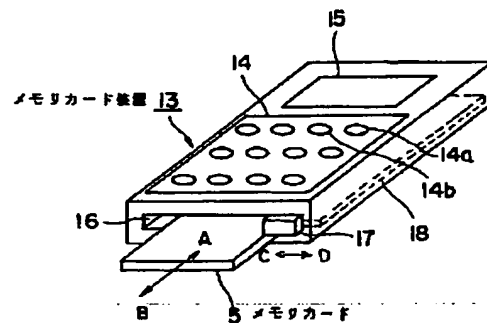
- 1 メモ리카ードライタ
- 3 AP媒体
- 5 メモ리카ード
- 8、30 秘密KEY
- 12、19 CPU
- 13 メモ리카ード装置
- 20 ROM
- 21 RAM

【図 1】



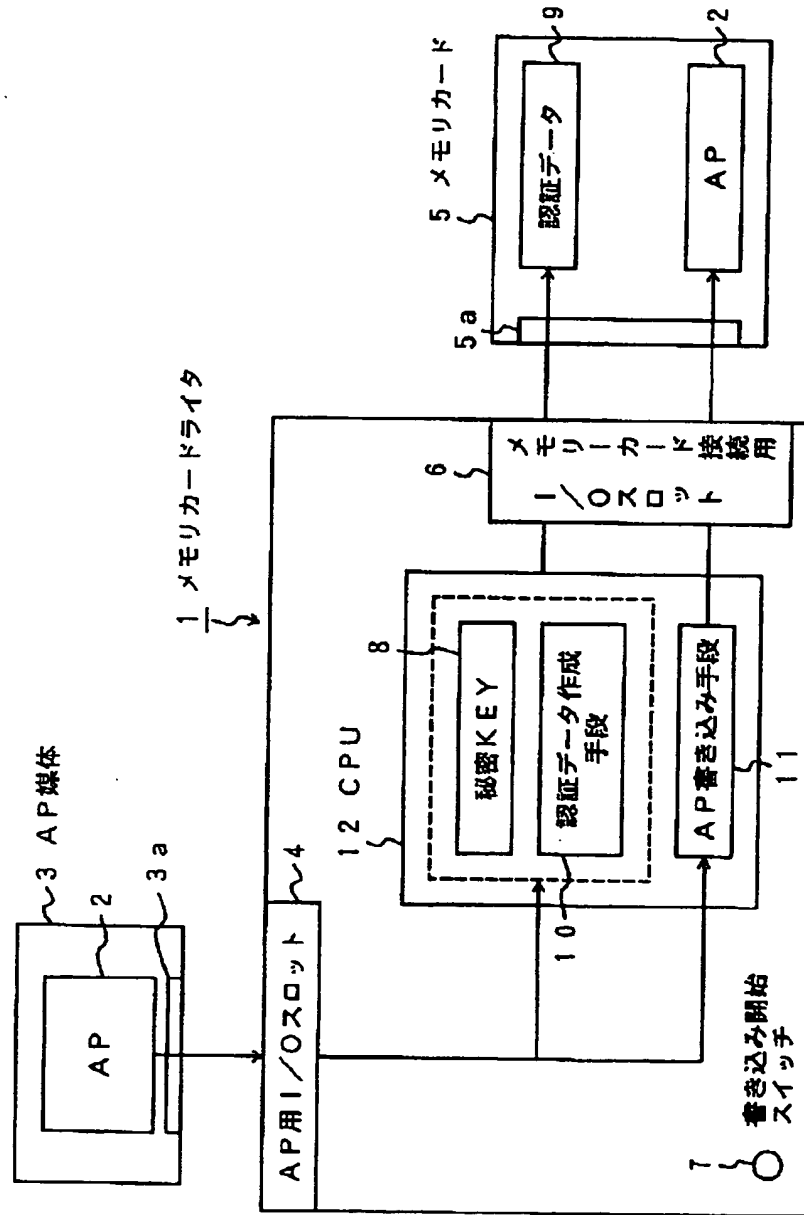
メモ리카ード認証動作の説明図(1)

【図 3】



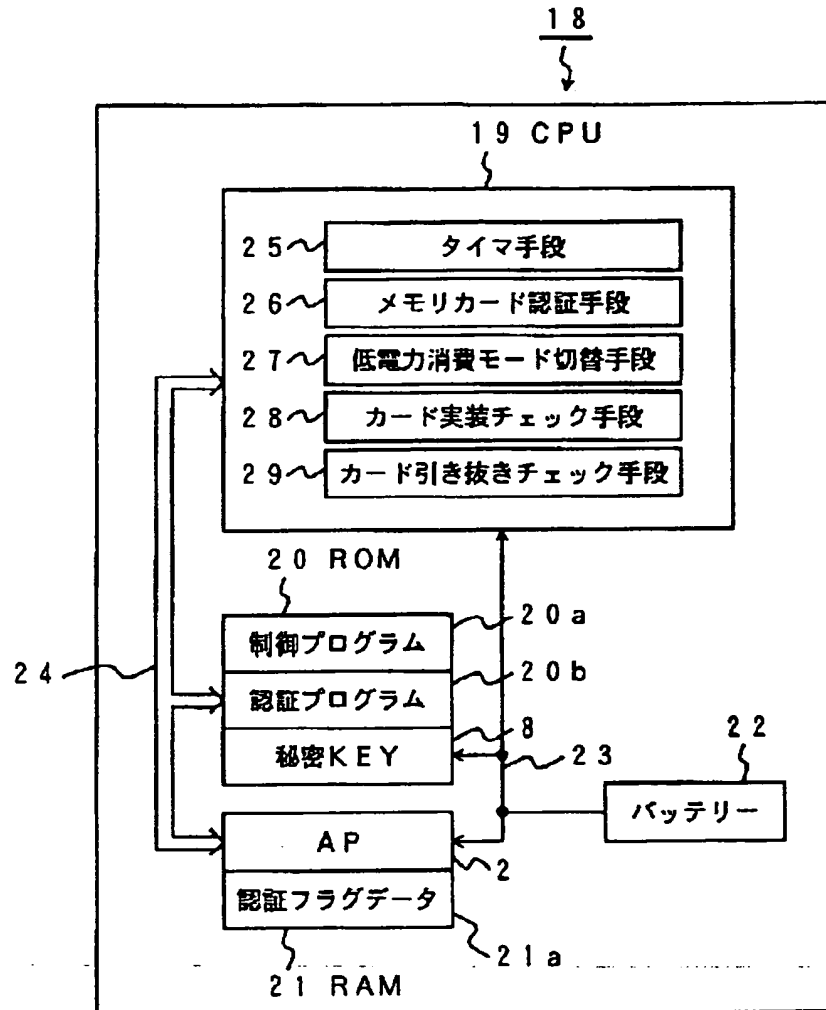
メモ리카ード装置の外観斜視図

【図2】



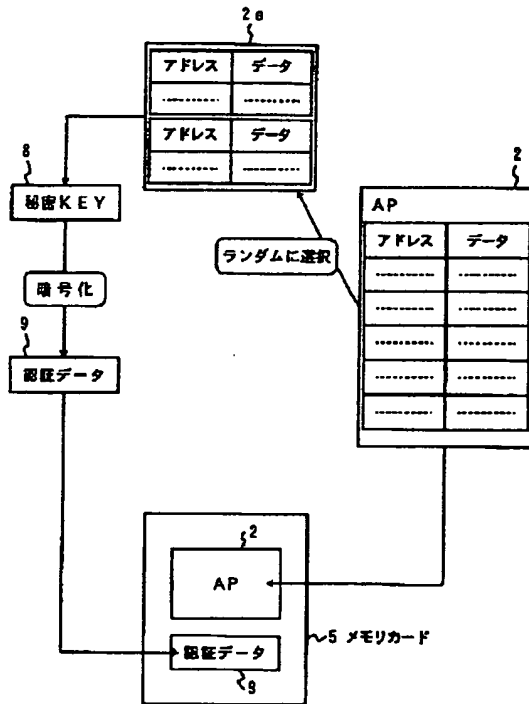
メモリカードドライタの構成を示すブロック図

【図4】



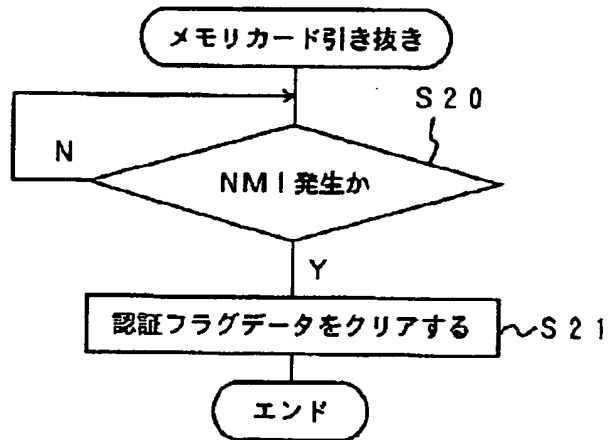
メモリカード装置に搭載される制御ブロック図

【図5】



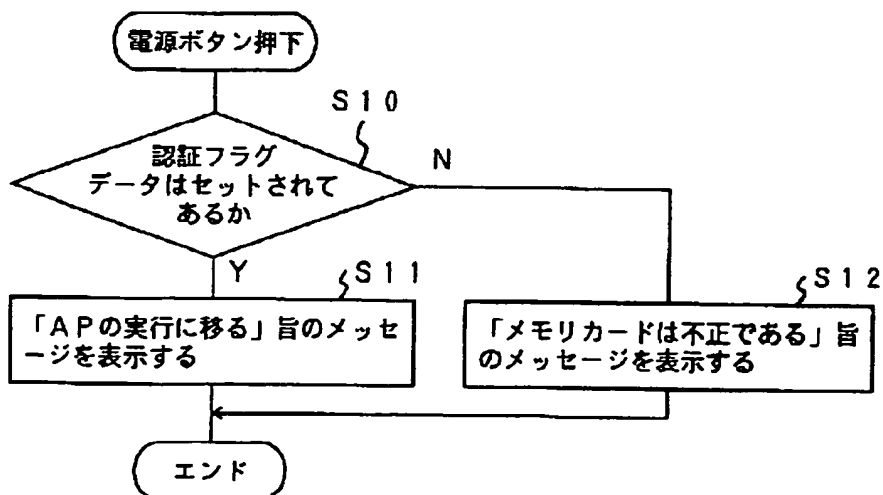
メモリカードライタの動作を示す説明図

【図8】



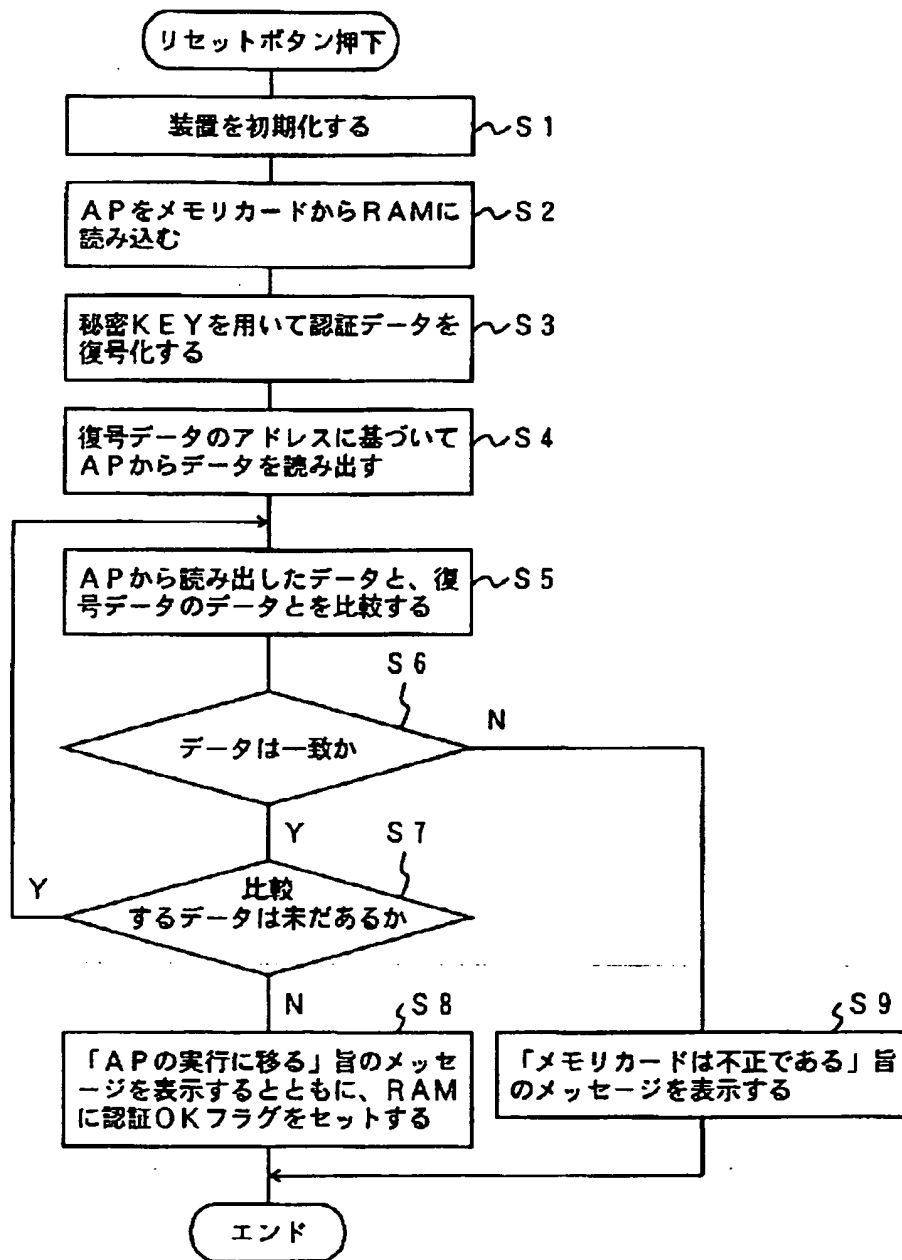
カード引き抜き後の動作を示すフローチャート

【図7】



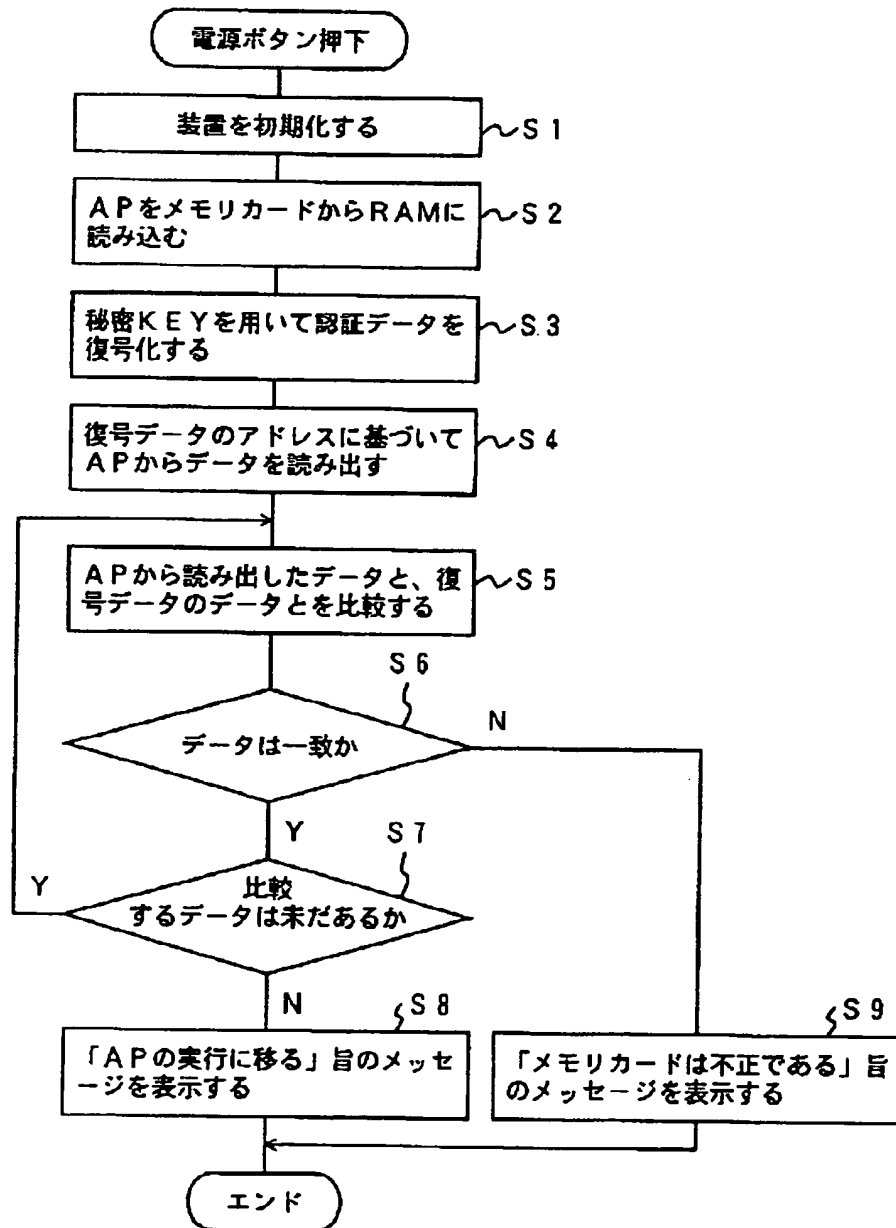
電源ボタン押下後の動作を示すフローチャート

【図6】



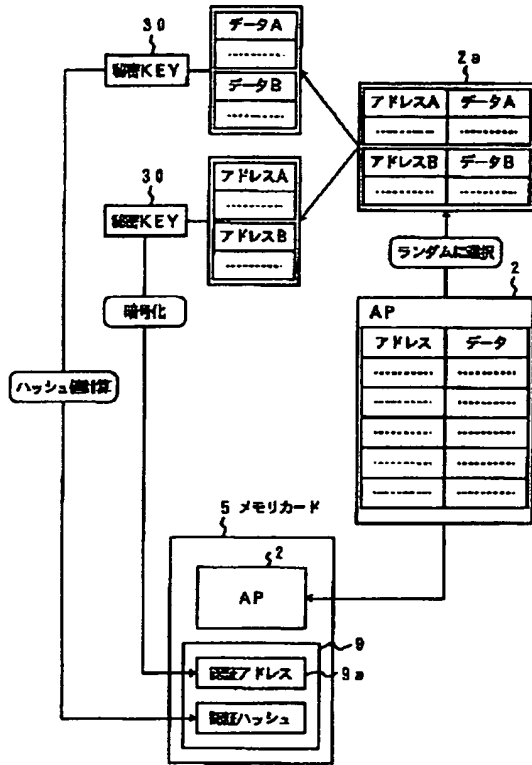
リセットボタン押下後の動作を示すフローチャート(1)

【図9】



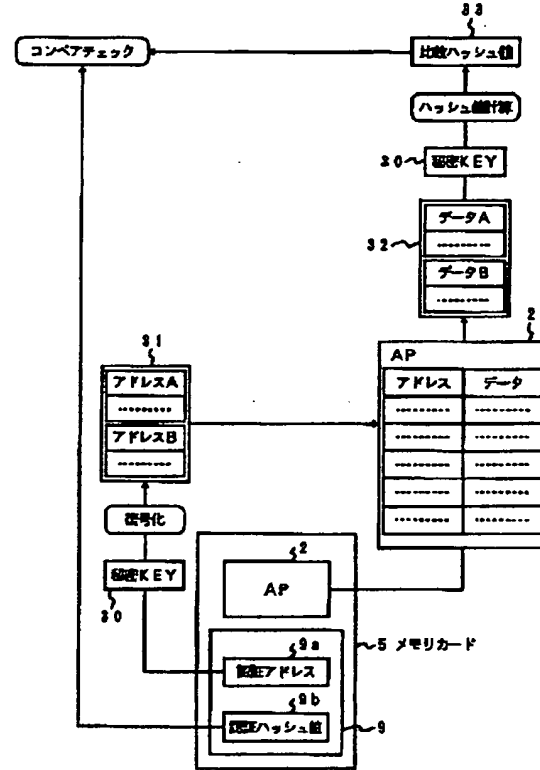
リセットボタン押下後の動作を示すフローチャート(2)

【図 10】



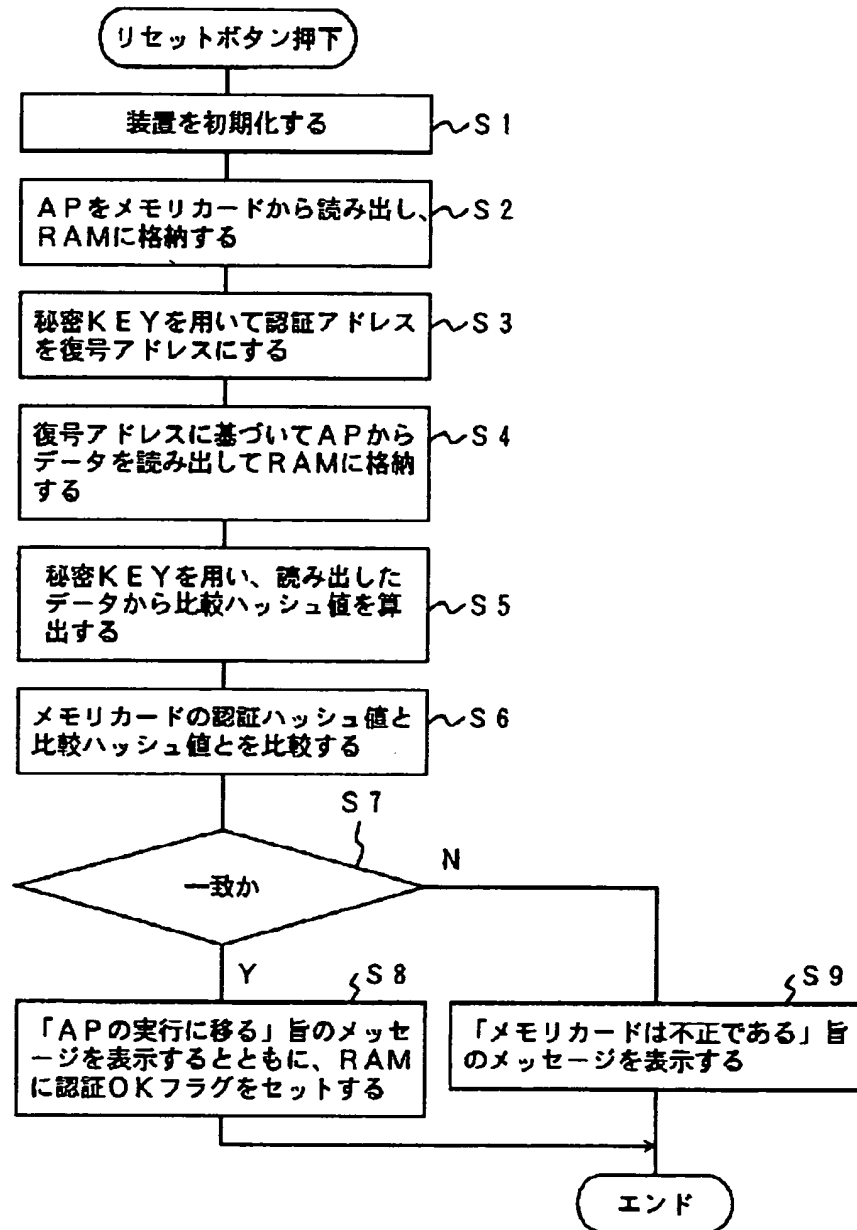
メモリカードライタの動作を示す説明図

【図 11】



メモリカード読取動作の説明図

【図 12】



リセットボタン押下後の動作を示すフローチャート(3)